

#5/ 4-20-02

BOX PATENT
Attorney Docket No.: 24698

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Group Art Unit: 2131

Jian Kang WU, et al.

Serial No. 09/904,651

Filed: July 16, 2001

For: **REMOTE PRINTING OF SECURE AND/OR AUTHENTICATED DOCUMENTS**

TRANSMITTAL LETTER

Commissioner for Patents
Washington, D.C. 20231

Sir:

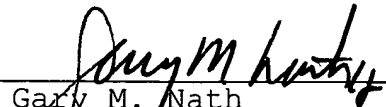
Submitted herewith for filing in the U.S. Patent and Trademark Office is the following:

- (1) Transmittal Letter
- (2) Request for Priority
- (3) Priority documents No. 200005827-1

Respectfully submitted,

NATH & ASSOCIATES PLLC

By:


Gary M. Nath
Registration No. 26,965
Customer No. 20529

Date: February 7, 2002
NATH & ASSOCIATES PLLC
1030 15th Street N.W., 6th Floor
Washington, D.C. 20005
(202)-775-8383
(202)-775-8396 fax
GMN/lis:Priority.TRANS

RECEIVED
FEB 11 2002
Technology Center 2100



BOX PATENT
Attorney Docket No. 24698

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Jian Kang Wu, et al.

Serial No. 09/904,651

Filed: July 16, 2001

For: REMOTE PRINTING OF SECURE AND/OR AUTHENTICATED
DOCUMENTS

RECEIVED
FEB 11 2002
Technology Center 2100

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner of Patents
Washington, D.C. 20231

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date October 11, 2001, the filing date of the corresponding application filed in SINGAPORE, bearing Application Number 200005827-1.

A Certified Copy of the corresponding application is submitted herewith.

Respectfully submitted,

NATH & ASSOCIATES PLLC

Date: February 7, 2002

By: Gary M. Nath
Gary M. Nath
Registration No. 26,965
Customer No. 20529

NATH & ASSOCIATES PLLC
6TH Floor
1030 15th Street, N.W.
Washington, D.C. 20005
(202)-775-8383
GMN/lis (Priority)



**REGISTRY OF PATENTS
SINGAPORE**

This is to certify that the annexed is a true copy of the following
Singapore patent application as filed in this Registry.

Date of Filing : 11 OCTOBER 2000

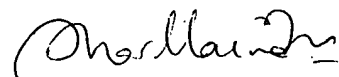
Application Number : 200005827-1

Applicant(s) : TRUSTCOPY PTE LTD

Title of Invention : REMOTE PRINTING OF A SECURE
AND/OR AUTHENTICATED DOCUMENTS

**CERTIFIED COPY OF
PRIORITY DOCUMENT**

RECEIVED
FEB 11 2002
Technology Center 2100



Sharmaine Wu Shee Mei
Assistant Registrar
for REGISTRAR OF PATENTS
SINGAPORE

**SINGAPORE
PATENTS ACT
(CHAPTER 221)
PATENTS RULES**

2 0 0 0 0 5 8 2 7 - 1


1 1 OCT 2000

The Registrar of Patents
Registry of Patents

REQUEST FOR THE GRANT OF A PATENT
THE GRANT OF A PATENT IS REQUESTED BY THE UNDERSIGNED ON THE BASIS OF THE PRESENT APPLICATION

I. Title of Invention	REMOTE PRINTING OF A SECURE AND/OR AUTHENTICATED DOCUMENTS	
II. Applicant(s) (See note 2)	(a) Name	TRUSTCOPY PTE LTD
	Body Description/ Residency	A COMPANY INCORPORATED IN SINGAPORE
	Street Name & Number	C/O KENT RIDGE DIGITAL LABS, 21 HENG MUI KENG TERRACE
	City	SINGAPORE 119613
	State	-
	Country	SINGAPORE
	(b) Name	
	Body Description/ Residency	
	Street Name & Number	
	City	
	State	
	Country	
	(c) Name	
	Body Description/ Residency	
	Street Name & Number	
	City	
	State	
	Country	

III. Declaration of Priority (see note 3)	Country/Country Designated	-	File no.		-	
	Filing Date	-	-	-		
	Country/Country Designated	-	File no.		-	
	Filing Date	-	-	-		
	Country/Country Designated	-	File no.		-	
	Filing Date	-	-	-		
IV. Inventors (See note 4)						
(a) The applicant(s) is/are the sole/joint inventor(s).		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No				
(b) A statement on Patents Form 8 is/will be furnished.		<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No				
V. Name of Agent (if any) (See note 5)		ALBAN TAY MAHTANI & DE SILVA				
VI. Address for Service (See note 6)		Block/Hse No	-	Level No	-	
		Unit No/PO Box	0643	Postal Code	911722	
		Street Name	-			
		Building Name	-			
VII. Claiming an earlier filing date under section 20(3), 26(6) or 47(4). (See note 7)		Application No	-			
		Filing Date	-	-	-	
		[Please tick in the relevant space provided]: () Proceeding under rule 27(1)(a). Date on which the earlier application was amended = _____ Or () Proceeding under rule 27(1)(b).				

VIII. Invention has been displayed at an International Exhibition (See note 8)		<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
IX. Section 114 requirements (See note 9)		The invention relates to and/or used a micro-organism deposited for the purposes of disclosure in accordance with section 114 with a depository authority under the Budapest Treaty. <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
X. Check List (To be filled in by applicant or agent)	A. The application contains the following number of sheet(s):-		
	1. Request	4	Sheets
		16	Sheets
	3. Claim(s).	4	Sheets
	4. Drawing(s).	4	sheets
	5. Abstract.	1	sheets
	B. The application as filed is accompanied by:-		
	1. Priority document		
	2. Translation of priority document		
	3. Statement of Inventorship & right to grant	X	
4. International Exhibition Certificate			
XI. Signature(s) (See note 10)	Applicant (a)		
	Date	11 OCTOBER 2000	
	Applicant (b)		
	Date		
	Applicant (c)		
	Date		

NOTES:

1. This form when completed, should be brought or sent to the Registry of Patents together with the prescribed fee and 3 copies of the description of the invention, and of any drawings.
2. Enter the name and address of each applicant in the spaces provided at paragraph II. Names of individuals should be indicated in full and the surname or family name should be underlined. The names of all partners in a firm must be given in full. The place of residence of each individual should also be furnished in the space provided. Bodies corporate should be designated by their corporate name and country of incorporation and, where appropriate, the state of incorporation within that country should be entered where provided. Where more than 3 applicants are to be named, the names and address of the fourth and any further applicants should be given on a separate sheet attached to this form together with the signature of each of these further applicants.
3. The declaration of priority at paragraph III should state the date of the previous filing, the country in which it was made, and indicate the file number, if available. Where the application relied upon in an International Application or a regional patent application e.g. European patent application, one of the countries designated in that application [being one falling under the Patents (Convention Countries) Order] should be identified and the name of that country should be entered in the space provided.
4. Where the applicant or applicants is/are the sole inventor or the joint inventors, paragraph IV should be completed by marking the 'YES' Box in the declaration (a) and the 'NO' Box in the alternative statement (b). Where this is not the case, the 'NO' Box in declaration (a) should be marked and a statement will be required to be filed on Patents Form 8.
5. If the applicant has appointed an agent to act on his behalf, the agent's name should be indicated in the spaces available at paragraph V.
6. An address for service in Singapore to which all documents may be sent must be stated at paragraph VI. It is recommended that a telephone number be provided if an agent is not appointed.
7. When an application is made by virtue of section 20(3), 26(6) or 47(4), the appropriate section should be identified at paragraph VII and the number of the earlier application or any patent granted thereon identified. Applicants proceeding under section 26(6) should identify which provision in rule 27 they are proceeding under. If the applicants are proceeding under rule 27(1)(a), they should also indicate the date on which the earlier application was amended.
8. Where the applicant wishes an earlier disclosure of the invention by him at an International Exhibition to be disregarded in accordance with section 14(4)(c), then the 'YES' Box at paragraph VIII should be marked. Otherwise the 'NO' Box should be marked.
9. Where in disclosing the invention the application refers to one or more micro-organisms deposited with a depository authority under the Budapest Treaty, then the 'YES' Box at paragraph IX should be marked. Otherwise the 'NO' Box should be marked.
10. Attention is drawn to rules 90 and 105 of the Patent Rules. Where there are more than 3 applicants, see also Note 2 above.
11. Applicants resident in Singapore are reminded that if the Registry of Patents considers that an application contains information the publication of which might be prejudicial to the defence of Singapore or the safety of the public, it may prohibit or restrict its publication or communication. Any person resident in Singapore and wishing to apply for patent protection in other countries must first obtain permission from the Singapore Registry of Patents unless they have already applied for a patent for the same invention in Singapore. In the latter case, no application should be made overseas until at least 2 months after the application has been filed in Singapore.

For Official Use

Application Filing Date: / /

Request received on : / /

Fee received on : / /

Amount :

*Cash/Cheque/Money Order No:

*Delete whichever is inapplicable

REMOTE PRINTING OF A SECURE AND/OR AUTHENTICATED DOCUMENTS

Field of the Invention

This invention relates to a method and apparatus for the remote printing of a secure and/or authenticated document and refers particularly, though not exclusively, to such a method and apparatus including controls over the printing process.

Definitions

Throughout this specification a reference to a document is to be taken as including a document in electronic or printed form.

Throughout this specification reference to authentication includes secure, and vice versa.

Background to the Invention

Paper documents are normally used to conduct business, and for administrative purposes. Despite the predictions repeatedly made for the paperless office, the digital age has seen an increase in the use of paper within offices. The main reason for this is trust. When a document is properly signed by an authorized person, their signature provides its authenticity. Wherever or on whatever the signature appears, one can proceed with some degree of certainty that the document is genuine. With the number of original documents being strictly controlled, and known, security is achieved.

Consideration of the Prior Art

US patent 6,091,507 relates to a method and apparatus for printing a document over a network. It deals with a network protocol, transmission format, and hardware interface facilitating high speed transmission of raster data from a host computer having a raster image processor, to a printer. Clearly, it does not address a number of important issues which are relevant for a document which is secure, trusted or authenticated.

US patent 5,983,065 relates to a method of printing secure documents. It uses a controlled access electronic printing machine to print original documents. The printed images formed thereby are recognizable in visible light, and arise from marking materials (liquid inks and/or dry toners) containing at least one photoactive (courmarin) compound. The original document images printed cannot be copied or scanned in a normal copier, or scanner. It uses special printing materials.

US patent 5,917,996 discloses a method to print a tamper-resistant form using tamper-resistant, composite electronic form characters, which overlay a security background.

US patent 6,085,181 is for a postage metering system for a stand-alone meter operating as a meter server on a network. Printer modules operate as client printer modules on the network coupled with a postal security device (PSD). The PSD includes unique identification, postal value storage and a digital signature generator. The client printer requests evidence of postage payment from the PSD through the local client printer module for concluding postage metering transactions. The evidence of postage payment includes a digital signature corresponding to each request for evidence of postage payment. This patent addresses usage control for postage.

In all of the prior art there is no disclosure addressing two most important issues: the control of number of copies made of a document, and control of the authenticity of the document.

Objects of the Invention

It is the principal object of the present invention to provide a method and apparatus for the remote printing of an authenticated document, the printing being able to be controlled.

Summary of the Invention

With the above and other objects in mind, the present invention provides a method for the remote printing of a document by use of a network, the method including the steps of:

- (a) receiving at a server the document as sent from a sender;

- (b) the server forwarding the document to a recipient;
- (c) the document being authenticated prior to being forwarded to the recipient; and
- (d) the server receiving instructions from the sender regarding printing controls and the server implementing those controls at the recipient.

The recipient may include a printer, the sender providing the printing controls to the printer for the printing of the document. The server may also be a trusted agent to the sender in printing control. The server preferably enables a secure document delivery from the sender through the server to the recipient. The server may also be a trusted third party for document verification. To do this the server may use hash and content feature of the document stored in the server. The secure document delivery and printing control may be based on a trusted document structure including one or more from the group consisting of:

- a) the document itself;
- b) a hand signature and/or seal of the sender;
- c) digital signature of each of the sender, recipient and the server system;
- d) optical watermark;
- e) content features of the document; and
- f) usage control and audit trail.

The sender may be the one who authenticates the document. The method may use a Public Key Infrastructure to provide nonrepudiation, privacy and security in the delivery of the document. The document can be encrypted at the sender's site using a public key of the recipient, and the digital signature of the sender may be applied to the document before being sent by the sender. A digital signature of the server can also be applied to the document before the document is sent by the server, and a digital signature of the recipient may be applied to the document when the document is received by the recipient. A document hash can be used as the digital signature and sent with document for validation, and hash and content feature of the document are kept in the server system for future verification.

The method may use a secure document transfer channel provided by Secure Socket Layer protocol, and authentication of the sender and the recipient may be by using user identity and at least one password.

The method may also use encryption techniques for secure document delivery. A key to decrypt the document can therefore be sent directly to the recipient by a carrier means selected from the group consisting of: email, telephone, mail, courier and personal delivery.

The document may be authenticated using an authentication means selected from the group consisting of: optical watermark, special ink, special paper and special printing materials.

The optical watermark may have a counterfeit-proof layer. The printer may be calibrated to achieve a high level of performance of the counterfeit-proof layer. The calibration may be performed using printing language without manual intervention. Also, the printer may be secure in the printing control process; and may include a secure memory, a secure central processing unit, and a secure clock. The secure memory may be used to store a private key, and at least one program; the central processing unit may be used to prevent run-time attacks; and the secure clock can be used to keep time. Preferably, the printer and the server use a public key pair, the printer and the server system performing secure handshaking to authenticate each other.

The server may send an encrypted document hash and optical watermark, and printing instructions, to the printer.

The printer may receive the document from client software, and verify the document with a hash and optical watermark before printing.

Preferably, the printer deletes the document immediately after printing; and an audit trail record is created in the server.

The recipient maybe trusted in the printing control process. In this case the server may communicate with the printer to verify the printer serial number and internet protocol address, check the status of the printers, lock a control panel of the printer, set all necessary printer settings, send instructions and the document for printing, reset printer settings after the printing process is completed, and create an audit trail record in the server.

Description of the Drawings

In order that the invention may be fully understood and readily put into practical effect there shall now be described by way of non-limitative example only preferred forms of the present invention, the description being with reference to the accompanying illustrative drawings in which:

Figure 1 is a block diagram of the document delivery and printing system;

Figure 2 depicts the structure of a trusted document; and

Figure 3 is a flow diagram for controlling a printer using PJI language.

Description of Preferred Embodiment

The present invention has three major components: The overall document transfer and printing process where a server system plays a role of trusted third party, means to authenticate the printed document, and the printing control itself.

Overall document transfer and printing process

To refer to Figure 1, there are four major components in a secure remote document printing system. The sender of the document should be a person authorized to initiate the document. The communication server system consists of at least one server which provides the necessary facilities for secure and reliable document delivery. It acts as a trusted third party in authenticating the sender, and the recipient, in the transaction based on the internal public key infrastructure (PKI) protocol. It also acts as a trusted agent, on behalf of the sender, to enforce the sender's printing requirements, and to control the printing process. The printing process is controlled by the communication server system through software residing at the recipient's site. For secure document delivery using encryption technology, please refer to ISO/CCITT X.400, and for PGP, see, for example, Network Security – private communication in a public world, by C. Kaufman, R. Perlman, and M. Speciner, PTR Prentice Hall, 1995.

During the transfer of the document, the document will have a structure such as that shown in Figure 2, which will make it a trusted document. Together with the document itself, there are other five items to be included:

- the hand signature and/or seal of the issuing authority to give people an immediate feeling of trust. The hand signature and seal is added to the document only if the authentication of the authority is successful. In that way, the hand signature is meaningful;
- the digital signature of the document by the sender, recipient and the server system for nonrepudiation and content integrity. The digital signature is an encryption of the document hash with a private key. Digital signatures by all three parties will guarantee the nonrepudiation of origin, receipt, and delivery;
- an optical watermark on the document provides authentication of the document, and protects the document from copying and forgery;
- the content feature of the document is extracted from the whole document. It is used to verify the contents of the document, and to locate possible changes. It is stored in the server system for future document verification purpose;
- the usage control and audit trail record maintain the usage statement by the authority, and also determines the status of the execution of the copy controls. It is managed by the server system

There are three choices of procedures, each having different levels of security:

- a) high security procedure based on PKI infrastructure. It provides a means for user authentication and nonrepudiation;
- b) secure delivery using Secure Socket layer (SSL) protocol; and
- c) secure delivery using encryption.

High security procedure based on PKI infrastructure

Registration

All users (senders and recipients) register with the service center, which runs the communication server system. The registration procedure includes, but may not be limited to:

- the user requests to be enrolled, and provides their identification, user identity ("ID"), type of service requested, and a digital certificate obtained from a public certification authority (if available).
- the service center then verifies the user's credentials, creates a user profile and stores the user profile in its registration database. The service center then generates a registration identity and transfers the information as well as trusted client software to the user. If the user does not have a digital certificate, the internal certification authority will issue a digital certificate to the user by the following steps:
 - the internal certification authority generates a message authentication code("MAC") key, and sends it to the user together with the client software and registration identity;
 - the user uses the client software to generate key-pair, generates a request for certification, encrypts it using the MAC key, and sends to the service center;
 - the service center then verifies the request, and signs and returns the user certificate. At the same time, the service center deposits a copy of the user certificate in the certificate database; and
 - the service center prints the user certificate's finger-print on hard copy, and both the service center and the registered user sign the hard copy.

Sending a document

If the sender wants to send a document to a recipient;

- the sender logs on to the server system by providing their login ID, and password;
- the server system verifies the sender ID and password and provides a prompt for the recipient's name, address, the document to be sent, and number of copies allowed to be printed by the recipient if the verification is successful. If the recipient with the requested ID exists on the service centre database, the server

system extracts the public key certificate from the certificate database, generates a unique serial number, and records the time of transaction. It is assumed that the time taken for entire process of the transaction can be ignored. If the recipient has not registered with the service center, the client software creates a session key, encrypts the data using the session key, encrypts the session key using a password, and sends the password by a separate email, telephone, or other means;

- the sender verifies the receiver's certificate, ID and the time of the transaction. The client software of the sender then computes the hash of the document to be sent, plus serial number, time, sender ID and recipient ID, signs these using the sender's private key, and sends it to the server system;
- the server system checks the signature's authenticity, and creates its own signature;
- the sender verifies the server system's signature, and incorporates it in the document;
- the client software of the sender adds to the document: hand signature of the user, seal of the sender's company, and the content feature of the document; encrypts the content feature and hash using the server system's public key, encrypts the rest of information and hash using the recipient's public key, and uploads it to the server system; and
- on receiving the encrypted document, the server system stores it in the evidence database and sends the recipient a notification. The hash and content feature are stored in the server for a predetermined period for document authentication purpose.

Receiving a document

Following the steps above:

- the server system advises the recipient of the availability of the document. A document ID and a serial number of the document is also sent;
- the recipient logs on to the server system with the recipient ID and password;

- the server system checks for validity, creates the hash of the document, hash serial number, time, sender ID and recipient ID. It signs these and sends the signature as well as the hash to receiver. The sender's public key, the encrypted document, and the sender's signature are also sent with this information;
- the receiver then validates the sender's public key certificate, decrypts the document, generates the hash and cross-checks with the generated hash sent by the server system. If they do match, the verification succeeds. The verification should also include the time of sending by the server system;
- the receiver's client software creates the signature of the hash of the document hash, serial number, recipient ID, and sender ID and time, and sends it to the server system. This will enable the service center to be fully convinced that the document has been successfully decrypted;
- the server system then verifies this information and stores the relevant information in the evidence database;
- when the recipient submits a request to print, the server system communicates with the printer at the recipient site via the client software and checks its status. If the printer is ready, the server system sends the document and the optical watermark for printing. Printing is successful if there is no error message. The server system creates an audit trail to record the entire process; and
- the server system sends an acknowledgement to the recipient, and notifies the sender.

Secure delivery using SSL

SSL (Secure Sockets Layer) protocol, as described in Transport Layer Security, version 1, RFC2246, 1999 provides a secure channel between two parties. All data transfer through the SSL channel will be encrypted using a session key. The session key is randomly generated for each connection. The sending steps are:

- the sender establishes a connection with the server system and securely negotiates a SSL session key. All transactions then pass through the encrypted channel;
- the sender logs on to the system with their login ID and password.

- the server verifies the sender identity through their login ID and password;
- the sender then submits a request to send data (which may be a document) to a recipient;
- the server acknowledges the request and prepares to receive the data;
- the sender sends the data together with the hash and content feature;
- on receiving the data, the server system stores it in the evidence database and sends the recipient a notification. The hash and content feature will be stored in the server for a predetermined period used for future authentication services;
- when the recipient receives the notification, with the client software they establish a connection with the server and negotiate a SSL session key;
- the recipient then logs on to the system with their login ID and password;
- the server verifies the recipient login ID and password. If verified, the server will deliver the data to the recipient;
- the recipient receives the data and sends an acknowledgement to server; and
- if the recipient submits a request to print an authenticated copy, the server will verify the document with the hash and content feature, communicate with the printer, and send the document as well as the optical watermark for printing. An audit trail is created to record the status of the entire process.

Secure Delivery Using Encryption

- sender logs in to server with their login ID and password;
- server verifies the sender login ID and password;
- sender submits request to send data (which again may be a document);
- server acknowledges the request and prepares to receive the data from the sender;
- sender creates a hash and a content feature from the data, and generates a random session key to encrypt the data. The key and the hash are encrypted using a password, the hash and the content feature are encrypted using server system's public key, and then are uploaded to the server system;
- server system receives the encrypted data, key, hash and content feature, stores them in the database;

- sender then informs the recipient through telephone, email, mail, personal delivery, or otherwise, of the password;
- when the recipient receives the password from the sender, the recipient logs in to the server with their login ID and password;
- server verifies the login ID and password. If verified, it will deliver the encrypted data, key and hash to the recipient;
- recipient receives the encrypted data, key and hash and sends an acknowledgement of receipt to the server;
- recipient decrypts the key and hash using the password obtained separately, and uses the key to decrypt the data;
- recipient computes the hash of the decrypted data and compares it with the received hash. If they are the same, another acknowledgement is sent to server; and
- if the recipient submits a request authority to print an authenticated document, the server system checks the database record of sender's definition to see if they are allowed to print the document, and how many copies they are allowed to print. If satisfactory, the server system verifies the document with the hash, communicates with the printer, and sends the document and the optical watermark for printing. An audit trail is created to record the status of the printing.

Means for document authentication

Any suitable means can be used for document authentication. For example, special inks and special paper can be used in a controlled way. Another example is to use an optical watermark with multiple layers of embedded image objects. The optical watermark image is stored in the server system, and transferred to the printer for printing on the document in a way controlled by the server system. An optical watermark on a document provides the authenticity in a sense that there is no optical watermark on the document if the document is printed without permission from the server system, and hence the document is not authenticated. The optical watermark is disclosed in our co-pending PCT application titled "Optical Watermark" filed in

Singapore on 15 September 2000, the contents of which are hereby incorporated by reference.

The optical watermark is to protect documents from counterfeiting and forgery. It embeds multiple latent image objects into layers of repetitive structures to generate a watermark. The watermark is then incorporated into a document as, for example, a seal, logo or background. This will be referred to as an "optical watermark".

The counterfeit-proof layer in the optical watermark is sensitive to the properties of the printer. Specifically, it depends on the size of the dots which are detectable by a photocopier. In order to guarantee the result of the printing of the optical watermark, a calibration process is necessary to determine the smallest visible dot size, and the best spatial frequency for its embedding. This process may include:

- generating an array of test patterns with different dot sizes;
- from the printed test page, the user locates the number of the first visible test pattern in order to find the smallest visible dot that the printer can print;
- based on this number, the system generates and prints an array of test patterns with different frequencies;
- from this printed page, the user determines the number of first invisible test pattern in order to find the frequency that can best hide the information;
- with the two numbers, a confirmation page is printed; and
- the user photocopies the confirmation page. If the anti-copy feature is seen, calibration is complete. Otherwise, the calibration is performed again until a successful result is obtained.

Printing control

The printing control provides a controlling process to ensure that the document is printed strictly according to the authority/sender's instruction. That is, the authority/sender inputs their instruction on the printing when they send the

document. The instruction is then implemented by the server system. As a trusted agent, the server system stores the instruction into the database as a part of document transfer history. The server system will control the printing process according to the instructions given by the sender. There are a number of ways in which the server system controls the printing process.

The existing printing process does not have any control. When the client gets the document from the server, it can be sent to a networked printer by a spool system. As soon as the printing request is in the queue of the spool, the link between the printing request and the client/server is severed. The only message is whether the printing request is successful or not. People can easily get hold of the data and require the printer to print multiple copies.

As the server system is trusted and secure, the server system communicates with the printer via client software. To ensure control of the printing process a number of methods may be used, which can include the recipient. The methods used will be different, and will be different again for an unsecured printer and/or non-secured recipient.

Printing control with a secure printer

A secure printer will have a hardware unit which includes of a clock; a secure memory to store encryption key, programs for encryption and decryption, and for data; a CPU to execute programs, to communicate with the client and the server, and to control the printer. This hardware unit is secure in a sense that it prevents attacks from outside to the clock, to the key and program, and to the run-time program. When a user requests authority to print an authenticated copy, the server system communicates with the printer to complete the handshaking process via the client. After successful authentication of the printer and the server system based on public key pairs, the server system sends the encrypted hash and optical watermark with time stamp, as well as printing instructions, to the printer. For the details on security handshaking protocols and encrypted data transmission, refer to Chapter 9

“Security Handshaking Pitfalls”, pp223 in the book of “Network Security – private communication in a public world”, by C. Kaufman, R. Perlman, and M. Speciner, PTR Prentice Hall, 1995.

The printer stores its private key in a secure memory. Its digital certificate is made known to the server system when the recipient is registered with the service center. After successfully completing the security handshaking process, the server system sends the encrypted instructions, document hash and optical watermark to the printer. All data is encrypted with a time stamp and digital signature. The printer receives the document from the client software, decrypts the data, verifies the digital signature and time stamp from the server, and prints it only if the verification is successful. The data is deleted immediately after printing. The printer creates hash of the printed data and signs the hash together with time stamp, and sends it to the server to be kept in the audit trail record.

With encryption technology and PKI infrastructure, the communication between the server system and the printer is secure. The secure printer is manufactured and inspected by a trusted manufacturer to ensure that the program stored in the secure memory cannot be tampered with, and to prevent run-time attacks on programs running in the CPU of the printer.

Printing Control with a trusted client

When the client is trusted, there should be no attack on the client software, or run-time attacks on the client software program. Through the client software, the server system communicates to the printer, checks its status, sends the printing instruction and data, monitors the whole process, and finally creates the audit trail record. The dialog with the printer uses available print task languages such as for example, PJJ and PML by Hewlett Packard. Figure 3 is a flow diagram of printing control using PJJ. The principal steps in the printing control process are:

- check and record the IP address and serial number of the printer;

- read the status of the printer, including the settings of the printer which are common to all print tasks, settings that are only valid to a specific print task, and the status of the printer at a fixed interval such as, for example, every 15 seconds;
- setting the values for all necessary settings required for the current printing task;
- locking of the control panel to prevent another user tampering with the settings while a print task is being sent to the printer. If the control panel is not able to be locked, the printing task is aborted; and
- sending of the print task using either PostScript (PS), Print Control Language (PCL), or Epson Standard Code for Printers (ESC/P).

The control program will first obtain all necessary information regarding the settings of the printer. With this information, undesired configurations or settings are reconfigured to desired settings. The printer is then set to report back the details of the device and page at a predetermined interval such as, for example, every 15 seconds. This is followed by the sending of the print task to the printer. With constant status reports, the printing process is closely monitored. If a genuine paper jam occurs, an error will be reported and a reprint can be performed. After printing is completed, the printer settings are reconfigured back to the original settings. All status reports will be captured for the audit trail.

The calibration process is not of necessity performed with manual intervention. That is, a calibration is carried out in the factory to compare visible dot size, and the toner level, and other printer parameters. With that data, and after the check of the printer status, a suitable printer setting is determined and set for the best performance of the optical watermark printed on the document.

Printing control with non-secure client with non-secure printer

A non-secure client or non-trusted client may mean possible attacks to client software and hardware, as well as the printer. These include attacks to the software, run-time attacks to obtain the data, and to provide false information to the server.

The attacker must have the skills to conduct those attacks. The main requirement is to have client software which is as attack-free as possible, or to introduce an extra hardware unit to protect the client software.

As can be seen, the present invention relates to the remote printing of an authenticated document which may have been transmitted over a network. This will avoid costly and slow physical delivery of the authenticated paper document. There are certain areas where the present invention may have considerably advantageous application. One is secure printing industries. They are a trusted and authorized agent. Authenticated documents, such as cash notes and bank checks, can be printed using special printers, special inks, special paper and other special materials. Both the printing process and printing materials are strictly controlled. The other is a signed document, where the authority initiates the document with their signature and/or seal. In both cases, the signature and special printing materials which add authenticity to the document are fully controlled by the authorized person or agent.

Whilst there has been described in the foregoing description preferred embodiments of the present invention, it will be understood by those skilled in the technical field that many variations or modifications in details may be made without departing from the present invention.

The claims

- 1) A method for the remote printing of a document by use of a network, the method including the steps of:
 - (e) receiving at a server the document as sent from a sender;
 - (f) the server forwarding the document to a recipient;
 - (g) the document being authenticated prior to being forwarded to the recipient; and
 - (h) the server receiving instructions from the sender regards printing controls and the server implementing those controls on the recipient.
- 2) A method for the remote printing a document by use of a network, the method including the steps of:
 - (a) a sender sending the document to a server to enable the server to forward the document to a recipient;
 - (b) the document being authenticated by the sender prior to sending it to the server; and
 - (c) sending to the server instructions for controlling the printing of the document to enable the server to implement those controls on the recipient.
- 3) A method for printing of an authenticated document received remotely by use of a network, the method including the steps of:
 - (a) a recipient receiving the authenticated document from a server, the server having received the authenticated document from a sender;
 - (b) the server providing implementation of printing controls on the recipient, the server having received the printing controls from the sender.
- 4) A method as claimed in any one of claims 1 to 3, wherein the recipient includes a printer, the server providing the printing controls to the printer for the printing of the document.

- 5) A method as claimed in any one of claims 1 to 4, wherein the server enables a secure document delivery from the sender through the server to the recipient.
- 6) A method as claimed in any one of claims 1 to 5, wherein the server is a trusted agent to the sender in printing control.
- 7) A method as claimed in any one of claims 1 to 6, wherein the server is a trusted third party in document verification services.
- 8) A method as claimed in claim 7, wherein the server uses hash and content feature of the document stored in the server.
- 9) A method as claimed in claim 7 or claim 8, wherein secure document delivery and printing control is based on a trusted document structure including one or more from the group consisting of:
 - a) the document itself;
 - b) a hand signature and/or seal of the sender;
 - c) a digital signature of each of the sender, recipient and the server system;
 - d) an optical watermark;
 - e) content features of the document; and
 - f) usage control and audit trail.
- 10) A method as claimed in any one of claim 7 to claim 9, wherein the sender authenticates the document.
- 11) A method as claimed in any one of claim 1 to 10, wherein the method uses a public key infrastructure to provide nonrepudiation, privacy and security in the delivery of the document.
- 12) A method as claimed in claim 10, wherein the document is encrypted at the sender's site using a public key of the recipient.
- 13) A method as claimed in claim 9 or claim 10, wherein a digital signature of the sender is applied to the document before being sent by the sender.
- 14) A method as claimed in any one of claims 11 to 13, wherein a digital signature of the server is applied to the document before the document is sent by the sender.

- 15) A method as claimed in any one of claims 11 to 14, wherein a digital signature of the recipient is applied to the document when the document is received by the recipient.
- 16) A method as claimed in any one of claims 11 to 15, wherein a document hash is used as a digital signature and sent with document for validation, and hash and content feature of the document are kept in the server system for future verification.
- 17) A method as claimed in any one of claims 1 to 10, wherein the method uses a secure document transfer channel provided by Secure Socket Layer protocol, and authentication of the sender and the recipient is by using user identity and at least one password.
- 18) A method as claimed in any one of claim 1 to 10, wherein the method uses encryption techniques for secure document delivery.
- 19) A method as claimed in claim 18, wherein a key to decrypt the document is sent directly to the recipient by a carrier means selected from the group consisting of email, telephone, mail, courier and personal delivery.
- 20) A method as claimed in any one of claims 1 to 19, wherein the document is authenticated using an authentication means selected from the group consisting of: optical watermark, special ink, special paper and special printing materials.
- 21) A method as claimed in claim 20, wherein the optical watermark has a counterfeit-proof layer.
- 22) A method as claimed in claim 21, including calibrating the printer to achieve a high level of performance of the counterfeit-proof layer.
- 23) A method as claimed in claim 22, wherein the calibration is performed using a printing language without manual intervention.
- 24) A method as claimed in any one of claims 4 to 23, wherein the printer is secure in the printing control process.
- 25) A method as claimed in claim 24, wherein the printer includes a secure memory, a secure central processing unit, and a secure clock.
- 26) A method as claimed in claim 25, wherein the secure memory is used to store a private key, and at least one program.

- 27) A method as claimed in claim 25 or claim 26, wherein the central processing unit is used to prevent run-time attacks.
- 28) A method as claimed in any one of claims 25 to 27, wherein the secure clock is used to keep time.
- 29) A method as claimed in claim 24, wherein the printer and the server use a public key pair, the printer and the server system performing secure handshaking to authenticate each other.
- 30) A method as claimed in claim 24, wherein the server sends the encrypted document hash, an optical watermark, and printing instructions, to the printer.
- 31) A method as claimed in claim 30, wherein the printer receives the document from client software, and verifies the document with a hash and time stamp, before printing and adds the optical watermark during printing.
- 32) A method as claimed in any one of claims 4 to 31, wherein the printer deletes the document immediately after printing.
- 33) A method as claimed in any one of claims 4 to 32, wherein there is included a final steps of creating an audit trail record in the server.
- 34) A method as claimed in any one of claims 4 to 33, wherein the recipient is trusted in the printing control process.
- 35) A method as claimed in claim 34, wherein the server communicates with the printer to verify the printer serial number and internet protocol address, check the status of the printer, lock a control panel of the printer, set all necessary printer settings, send to the printer instructions for printing, and the document reset settings after the printing process is completed, and to create an audit trail record in the server.

Abstract**REMOTE PRINTING OF A SECURE AND/OR
AUTHENTICATED DOCUMENTS**

A method for the remote printing of a document by use of a network, the method including the steps of:

- (a) receiving at a server the document as sent from a sender;
- (b) the server forwarding the document to a recipient;
- (c) the document being authenticated prior to being forwarded to the recipient; and
- (d) the server receiving instructions from the sender regards printing controls and the server implementing those controls on the recipient.

Figure 1

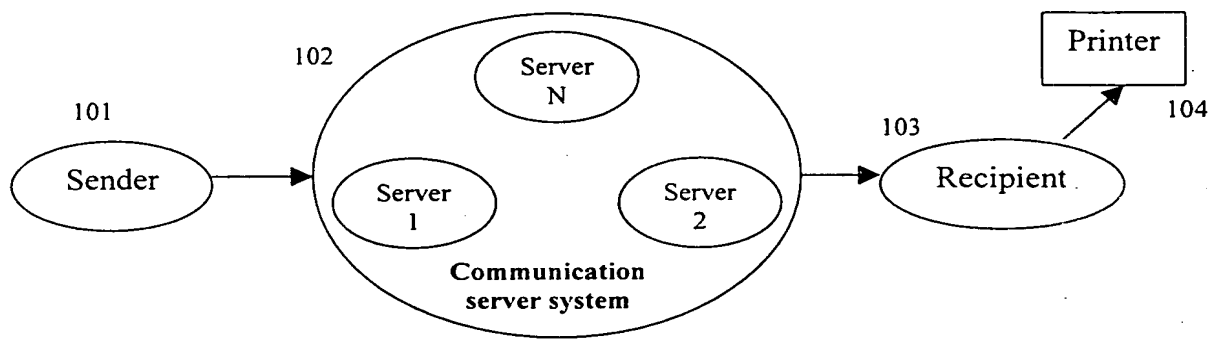


Figure 1

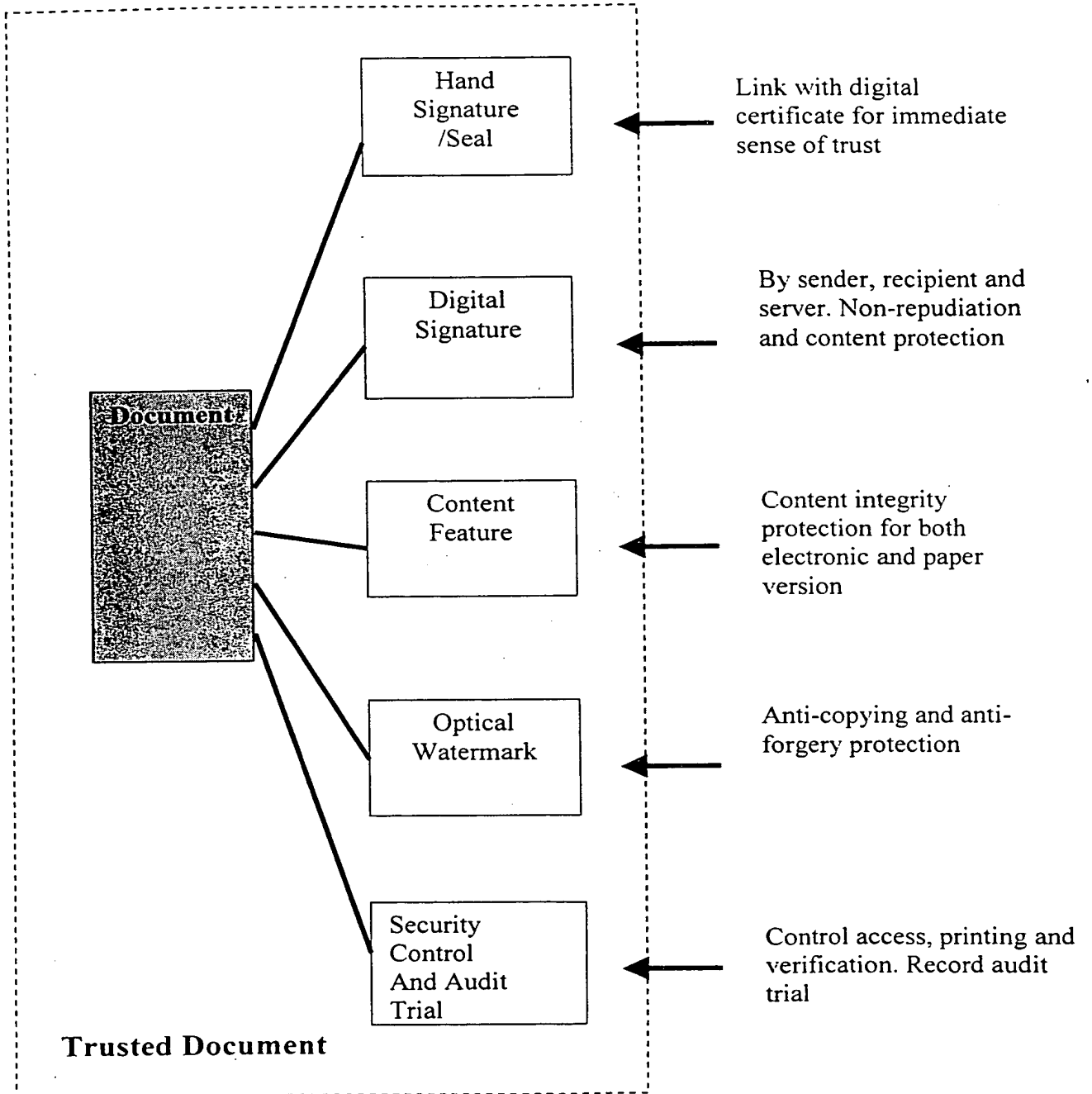


Figure 2

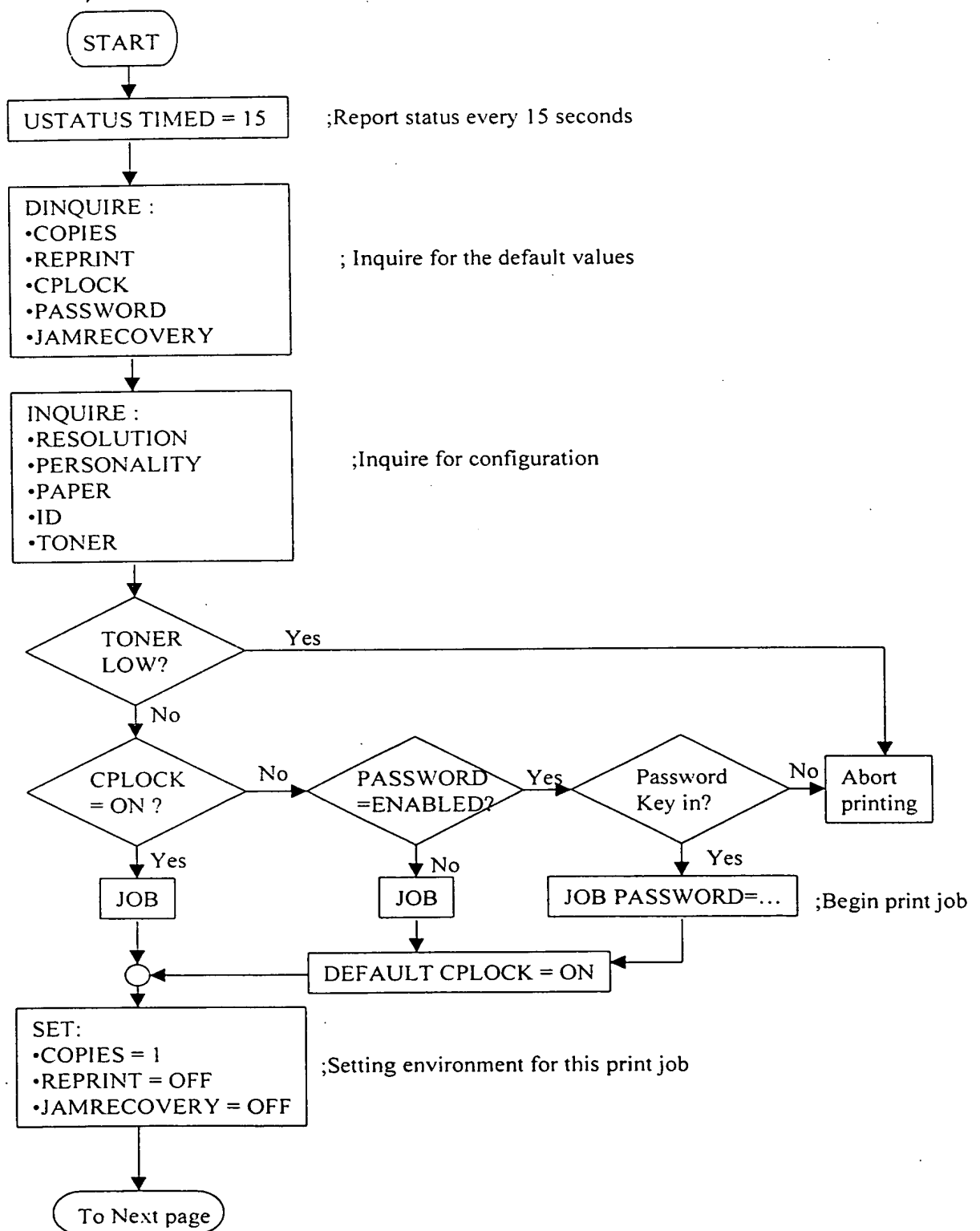


Figure 3, first part

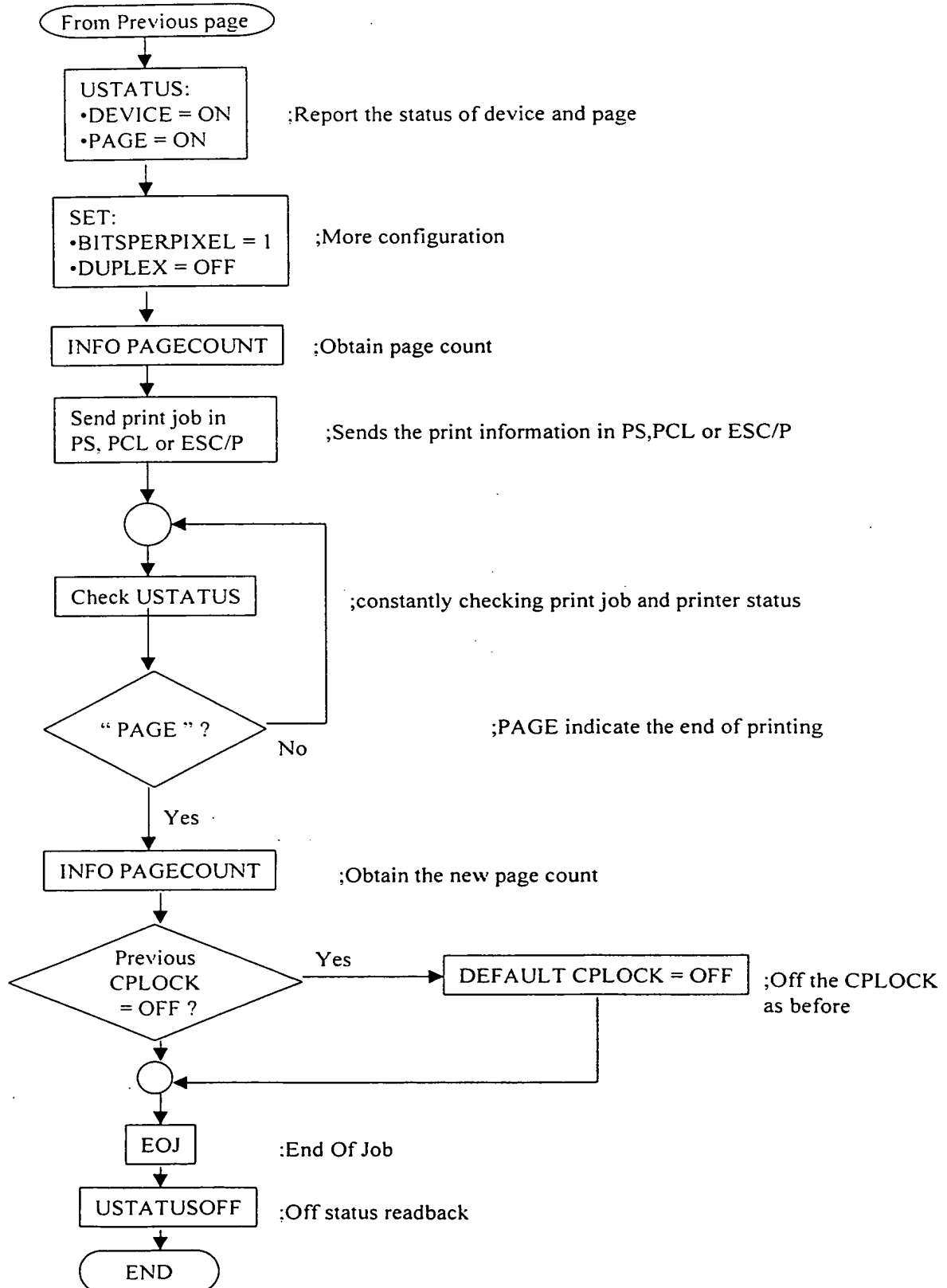


Figure 3, second part